

## Relationships among Differential , Truncated Differential and Impossible Differential Cryptanalyses against Word-Oriented Block Ciphers like Rijndael

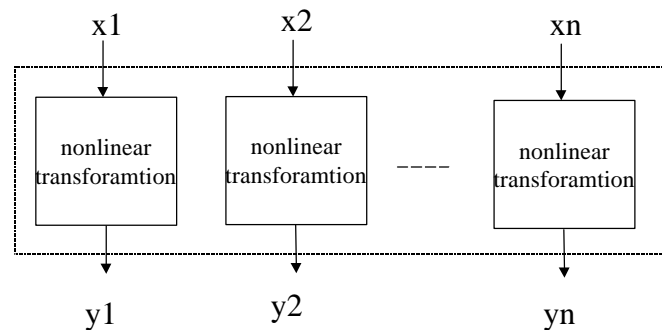
---

Makoto Sugita, Kazuhiro Uehara, Shuji Kubota  
NTT Network Innovation Laboratories  
Kazukuni Kobara, Hideki Imai  
University of Tokyo

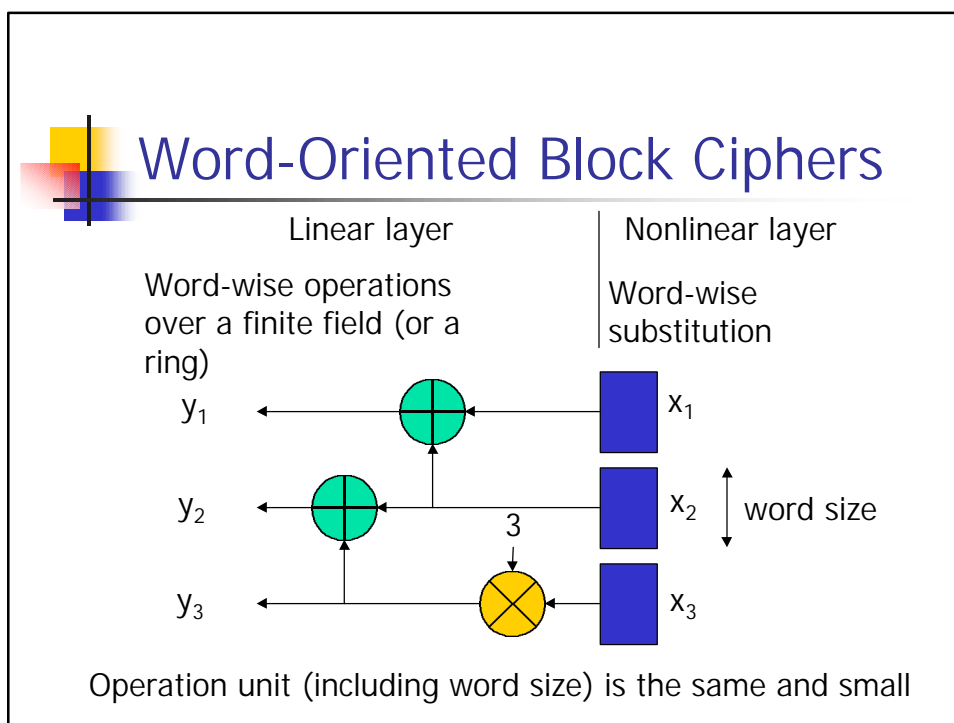
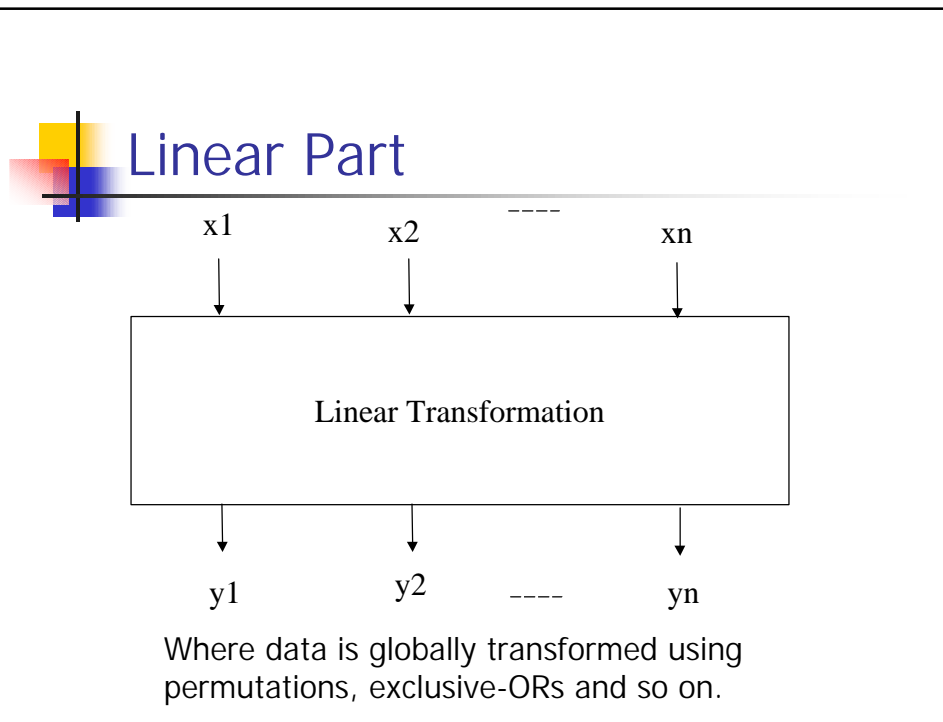


## Nonlinear Part

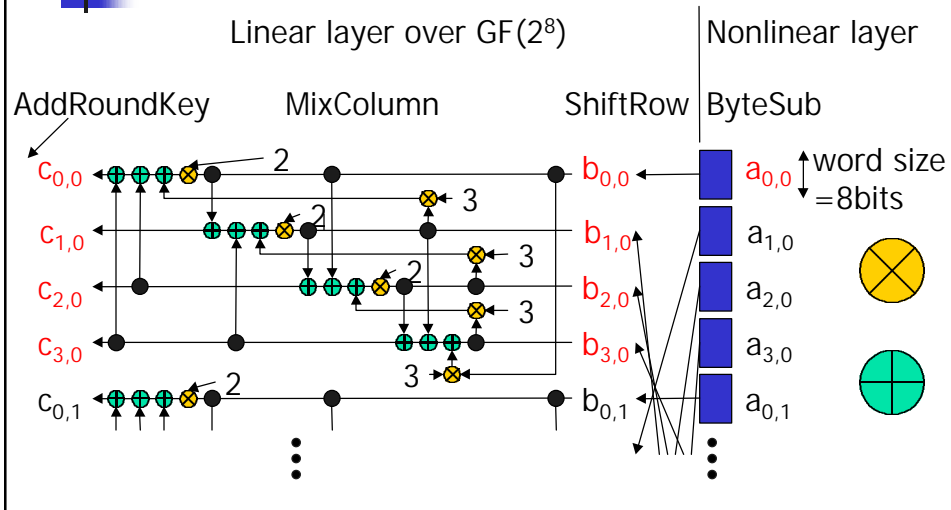
---



Where data is locally transformed using, e.g. S-boxes.



# Rijndael



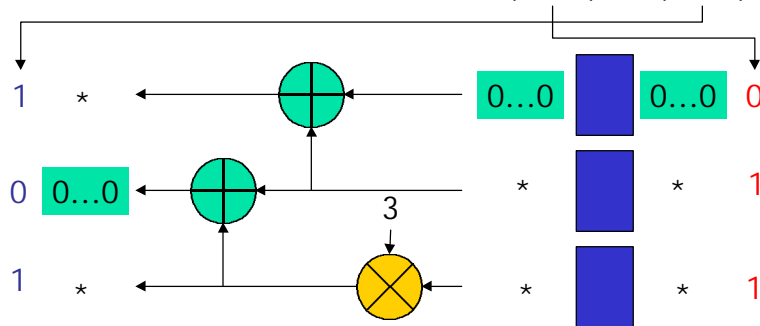
# Outline

- Proposal of an **efficient** algorithm to estimate **all the truncated differential probabilities** of the word-oriented block ciphers
  - where randomly chosen differentials are given.
- Evaluation of Rijndael
  - Truncated differential probabilities of single layer MixColumn
  - Impossible truncated differentials for multiple round Rijndael

## Truncated Differential Probability

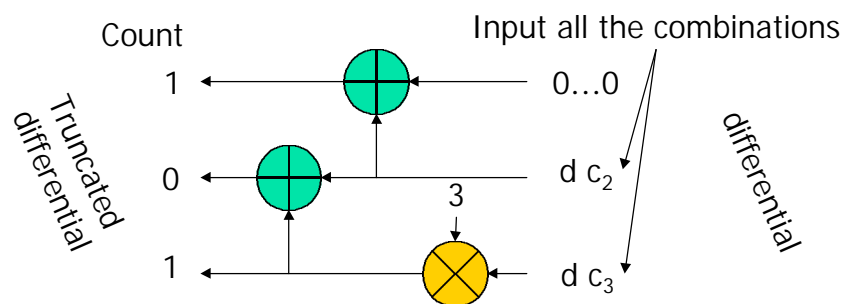
Some of the output byte-differentials happen to be 0 after some of the input byte-differentials are fixed to 0 and the other nonzero differentials are uniformly distributed.

Truncated differential:  $(0, 1, 1) \rightarrow (1, 0, 1)$



## Naive Method to Estimate All the Truncated Differential Prob.

- Input all the combinations of the nonzero differentials into the linear layer, one by one.
- Count the frequency of each output truncated differential pattern.



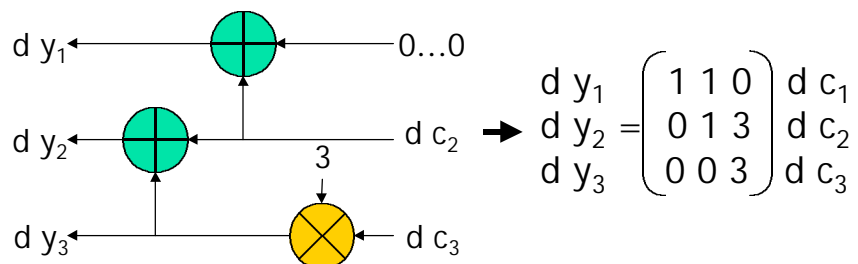
## Our Method

- Does the same thing with a small computational cost.

Outline of our algorithm

- Write down the linear layer in a matrix form.
- Make a constraint matrix.
- Calculate the rank of the matrix.
- Exclude overlapped combinations.

## Matrix Form



## Constraint 1

- Both input and output differentials must satisfy the following equation.

$$\begin{matrix} d y_1 \\ d y_2 \\ d y_3 \end{matrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 3 \end{pmatrix} \begin{matrix} d c_1 \\ d c_2 \\ d c_3 \end{matrix} \rightarrow \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} = \begin{pmatrix} 1 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 3 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & -1 \end{pmatrix} \begin{matrix} d c_1 \\ d c_2 \\ d c_3 \\ d y_1 \\ d y_2 \\ d y_3 \end{matrix}$$

## Constraint 2

- Consider the following truncated differentials.
- Both  $d c_1$  and  $d y_2$  must be 0.

Truncated differential

$$\begin{matrix} 1 \\ 0 \\ 1 \end{matrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 3 \end{pmatrix} \begin{matrix} 0 \\ 1 \\ 1 \end{matrix} \rightarrow \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} d c_1 \\ d c_2 \\ d c_3 \\ d y_1 \\ d y_2 \\ d y_3 \end{matrix}$$

Diagram illustrating the truncated differential equation. The input differentials are  $d c_1$  and  $d y_2$ , which are highlighted in red boxes. The output differentials are  $d c_2$  and  $d y_3$ , which are highlighted in blue boxes. The equation shows that the truncated differential is zero, leading to the constraints  $d c_1 = 0$  and  $d y_2 = 0$ .



## Constraint Matrix

$$\begin{array}{c}
 \begin{pmatrix} 1 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 3 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & -1 \end{pmatrix} \\
 \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}
 \end{array}
 \rightarrow
 \begin{array}{c}
 0 \\ 0 \\ 0 \\ 0 \\ 0
 \end{array}
 =
 \begin{pmatrix} 1 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 3 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}
 \begin{pmatrix} d\ c_1 \\ d\ c_2 \\ d\ c_3 \\ d\ y_1 \\ d\ y_2 \\ d\ y_3 \end{pmatrix}$$



## Rank

- Find the combinations satisfying the following constraints.

Rank=5      Dimension=6

$$\begin{array}{c}
 0 \\ 0 \\ 0 \\ 0 \\ 0
 \end{array}
 =
 \begin{pmatrix} 1 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 3 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}
 \begin{pmatrix} d\ c_1 \\ d\ c_2 \\ d\ c_3 \\ d\ y_1 \\ d\ y_2 \\ d\ y_3 \end{pmatrix}
 \left| \begin{array}{l}
 6 \text{ dimensions} \\
 -5 \text{ dimensional constraints} \\
 \hline
 = 1 \text{ free dimension}
 \end{array} \right.$$

$M = 2^{\text{word size} \times 1} \text{ combinations}$

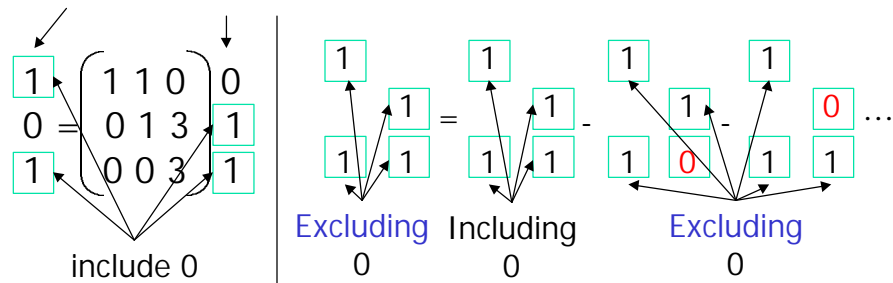


## Exclusion

- M includes the cases that some of the  s become 0.
- Excluding these cases, N is obtained.

Truncated differential

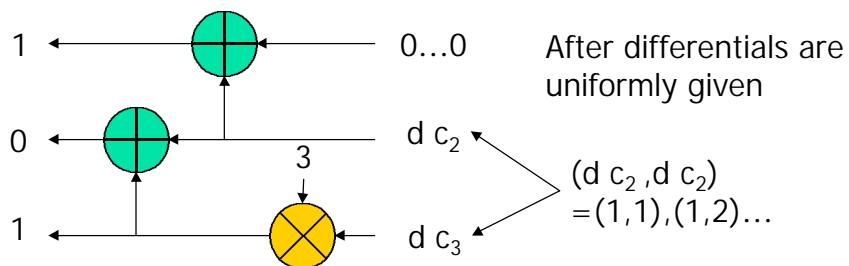
$$N = M - N1 - N2 \dots$$



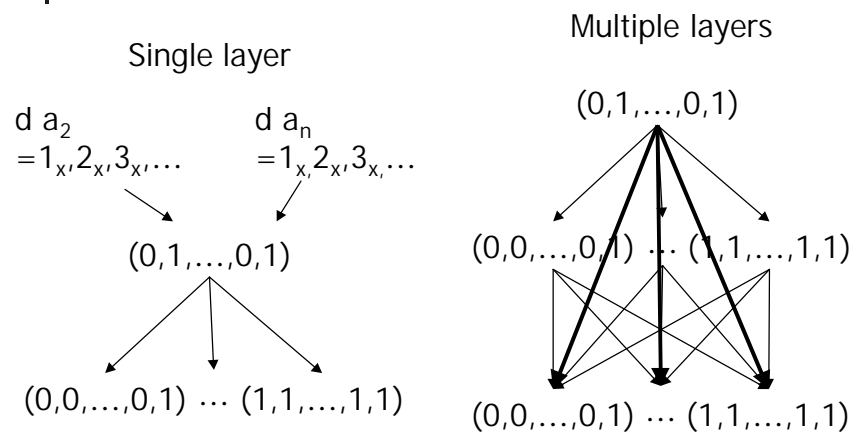
## Expected Value

Expected value of the truncated differential prob.

$$= \frac{N}{\text{The number of input combinations}}$$



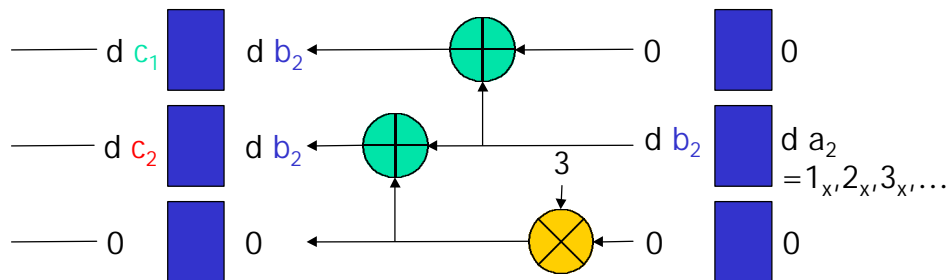
## Truncated Differential prob. for multiple layers



## Assumptions

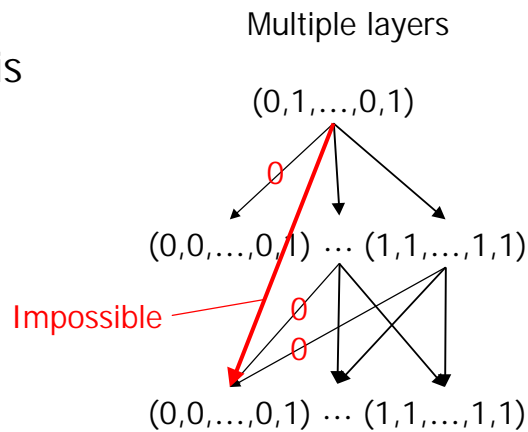
$(d c_1, d c_2)$  is uniform  
 $\{d c_1\}$  is independent of  $\{d c_2\}$   
 Not necessarily true

$d b_2$  is uniform  
 Can be true



## Impossible Truncated Differential for multiple layers

- Assumptions is not required
- Since the probability 0 remains 0 even if the assumption is false.



## Evaluation of Rijndael

- Truncated differential probability for
  - Single MixColumn
- Impossible truncated differentials for
  - Multiple round Rijndael

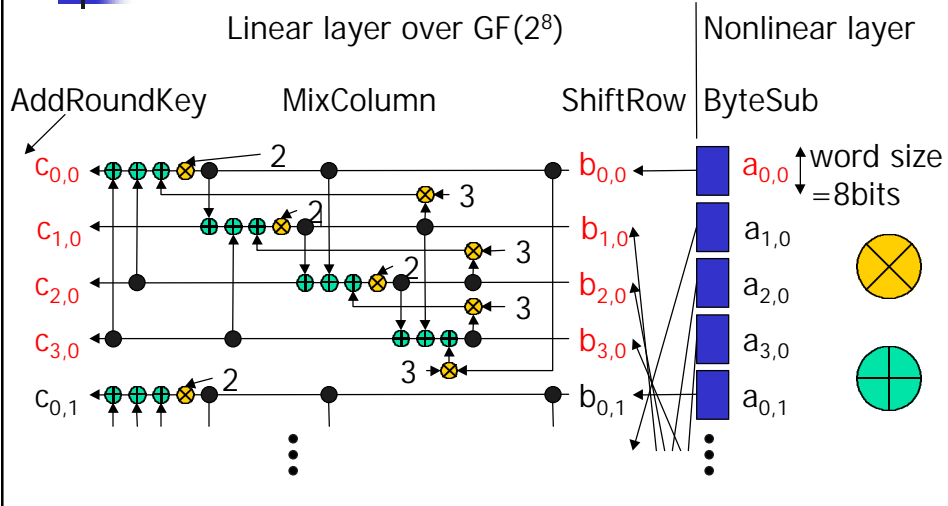
## Truncated Differential Probabilities for Single-layer 4-byte MixColumn

- Truncated differential prob. of 16-bytes is given by a direct product of these prob.

HW( $b_{00}, b_{10}, b_{20}, b_{30}$ )	HW( $c_{00}, c_{10}, c_{20}, c_{30}$ )	Prob.
1	1,2,3	0
1	4	1
2	1,2	0
2	3	p
2	4	251p

$$P = \frac{1}{2^8 - 1}$$

## Rijndael



## Truncated Differential Probabilities for Single-layer 4-byte MixColumn

HW( $b_{00}, b_{10}, b_{20}, b_{30}$ )	HW( $c_{00}, c_{10}, c_{20}, c_{30}$ )	Prob.
3	1	0
3	2	$p^2$
3	3	$251p^2$
3	4	$251p + 10p^2$
4	1	$p^3$
4	2	$251p^3$
4	3	$251p^2 + 10p^3$
4	4	$251p + 9p^2 + 235p^3$

$$P = 1/(2^8 - 1)$$

## Impossible Truncated Differentials

- Does not exist after 3 rounds when randomly chosen differences are given.
  - (3-round Rijndael is vulnerable by the impossible truncated differential attack. )

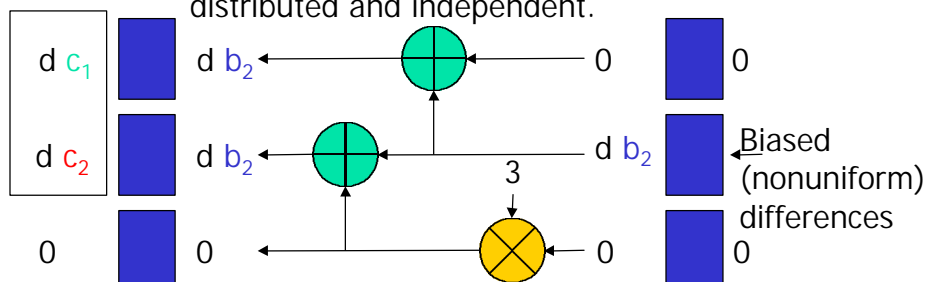
Rounds	Impossible Paths
2 (1 linear layer)	65534
3	14910
4	0

## Conclusion

- We proposed an **efficient** algorithm for estimating **all the truncated differentials** of the word-oriented block ciphers
  - Where randomly chosen differentials are given.
- We evaluated
  - Truncated differentia probabilities for single layer MixColmn
  - Impossible truncated differentials for multiple round Rijndael

## Further Work

- Evaluation of truncated diff. prob. after biased (nonuniform) differentials are given.
- Considering the validity of the assumptions we used for multiple layers.
  - Next layer's input differentials are uniformity distributed and independent.



## Cherry blossoms in Japan

